UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,704	08/07/2001	Peter Malcolm	112634.120	2337

28089 7590 02/09/2007		EXAMINER
WILMER CUTLER PICKERING HALE AND DORR LLP		ELISCA, PIERRE E
399 PARK AVENUE		
NEW YORK, NY 10022	ART UNIT	PAPER NUMBER
	3621	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	02/09/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 02/09/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

teresa.carvalho@wilmerhale.com
tina.dougal@wilmerhale.com
michael.mathewson@wilmerhale.com

	Application No.	Applicant(s)
~~Supplemental~~ Office Action Summary	09/923,704	MALCOLM, PETER
	Examiner	Art Unit	
	Pierre E. Elisca	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2006*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46,114-157,178-261,304-353,377-418,438-460 and 476-585* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☒ Claim(s) *See Continuation Sheet* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

Continuation of Disposition of Claims: Claims rejected are 1-8, 11-31, 34-46, 114, 115, 121, 124-137, 143-157, 178, 179, 181, 182, 184-191, 195, 205, 207-221, 223-227, 237, 247, 249-261, 304-311, 313-330, 336, 338- 353, 377, 378, 388- 399, 409-415, 417, 418, 438-445, 449-460, 476, 477, 483, 486-499, 501, 502, 505, 515, 525-551, 553-566 and 576-585 .
Continuation of Disposition of Claims: Claims objected to are 9, 10, 32, 33, 116-120, 122, 123, 138-142, 180, 183, 192-194, 196-204, 206, 222, 228-236, 238-246, 248, 312, 331-335, 337, 379-387, 400-408, 416, 446- 448, 478-482, 484, 485, 500, 503, 504, 506-514, 516-524, 552 and 567-575 .

DETAILED ACTION

1.   This office action is in response to Applicant's amendment filed on 08/03/2006.

Regarding the status of the claims in the instant application, the Examiner has found

new prior art. The Examiner is obliged to apply the newly found prior art. The Examiner

regrets the delayed process of the application. Accordingly, claims 1-46, 114-157, 178-

261, 304-353, 377-418, 438-460 and 476-585 are pending.

Allowable Subject Matter

2.   Claims 9, 10, 32, 33, 116-120, 122, 123, 138-142, 180, 183, 192-194,

196-204, 206, 222, 228-236, 238-246, 248, 312, 331-335, 337, 379-387, 400-408, 416,

446- 448, 478-482, 484, 485, 500, 503, 504, 506-514, 516-524, 552 and 567-575 are

objected to as being dependent upon a rejected base claim, but would be allowable if

rewritten in independent form including all of the limitations of the base claim and any

intervening claims.

Claim Objections

3.   Claim 329 is objected to because of the following informalities: Claim 329

recites the " may be", Applicant is advised to remove the word " may be" into the claims.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-8, 11-31, 34-46, 114, 115, 121, 124-137, 143-157, 178, 179, 181, 182,

184-191, 195, 205, 207-221, 223-227, 237, 247, 249-261, 304-311, 313-330, 336, 338-

353, 377, 378, 388- 399, 409-415, 417, 418, 438-445, 449-460, 476, 477, 483, 486-499,

501, 502, 505, 515, 525-551, 553-566 and 576-585 are rejected under 35 U.S.C. 103

(a) as being unpatentable over Shwed et al (U.S. Pat. No. 5,835,726) in view of Kaler et

al US 2003/0140282 A1.

As per claims 1, 5-8, 11-31, 34-46, 115, 121, 124-135, 137, 143-157, 178, 179, 181,

182, 184-191, 195, 205, 207-221, 223-227, 237, 247, 249-261, 304-311, 313-330, 336,

338- 353, 378, 388- 397,339, 409-415, 417, 418, 438-445, 449-460, 477, 483, 486-499,

501, 502, 505, 515, 525-551, 553-564, 566 and 576-585 Shwed discloses a

system/method for securing the flow of and selectively modifying packets in a computer

network by controlling the inbound and outbound, the system comprising:

A plurality of workstations adapted for connection to a computer network, each

workstation having a memory (see., figs 1 and 2, abstract, col 3, lines 8-67, col 4, lines

1-44, col 9, lines 1-67, col 10, lines 1-67);

A data repository arranged to receive data from each of said workstations (see.,

abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67);

An application stored in said memory of each workstation for transmitting outbound data

to said network and receiving inbound data from said network (see., figs 13 –15,

abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67);

Policy data containing rules defining relevant commercial data which is to be stored in

said data repository (see., col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10,

lines 1-67); and

policy data to monitor at least one of said outbound data and said inbound data, to

identify in at least one of said outbound data and said inbound data, relevant

commercial data that is to be stored in said data repository in accordance with said

rules in said policy data, and to cause said relevant commercial data to be stored in said

data repository (see., abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col

10, lines 1-67).

It is to be noted that Shwed fails to explicitly disclose that an analyzer, said analyzer

being operable in conjunction with said policy data. However, Kater discloses a

method/apparatus for analyzing the performance of a data processing system,

particularly a distributed data processing, system, provide a system user with tools for

analyzing and application running thereon (see., abstract, pages 1-11, [0096] and

[0116]. Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to modify the teaching of Shwed by including the

limitation detailed above as taught by Kater because this would analyze performance of

a data processing system.

As per claim 2, Shwed discloses the claimed limitation wherein said relevant data that is to be stored in said data repository is encrypted prior to it being transmitted to said data repository (see., figs 13-15, col 11, lines 25-67, col 12, lines 1-67, col 13, lines 1-28).

As per claim 3, Shwed discloses the claimed limitation wherein said relevant data that is stored in said data repository is encrypted (see., figs 13-15, col 11, lines 25-67, col 12, lines 1-67, col 13, lines 1-28).

As per claim 4, Shwed discloses the claimed limitation wherein said computer network, to which said one or more workstations are adapted for connection, is the Internet (see., figs 1 and 2).

As per claim 9, Shwed discloses the claimed limitation wherein said analyzer is operable to identify, as relevant data, digital certificates contained in at least one of said outbound or said inbound data or used to digitally sign signed data in said inbound data or said outbound data, or sufficient descriptive data to identify such digital certificates, said digital certificates and/or said descriptive data being stored in said data repository (see., abstract, lines 21-30).

As per claim 114 Shwed discloses a system/method for securing the flow of and selectively modifying packets in a computer network by controlling the inbound and outbound, the system comprising:

One or more workstations adapted for connection to a computer network, each

workstation having a memory; an application stored in said memory of each workstation

for transmitting outbound data to said computer network and receiving inbound data

from said computer network; policy data containing rules specifying an appropriate

encryption strength for outbound data, the encryption strength depending on the content

of the data; and appropriate strength for the outbound data; wherein said analyzer

controls transmission of said outbound data from said application in dependence upon

said determination of an appropriate encryption strength (see., figs 1 and 2, abstract, col

3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67).

It is to be noted that Shwed further discloses an encryption strength see., col 2,

lines 37-40, col 13, lines 7-19, specifically wherein said the modification of

packets by, e.g., encryption of outbound packets....).

Policy data containing rules defining relevant commercial data which is to be stored in

said data repository (see., col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10,

lines 1-67); and

policy data to monitor at least one of said outbound data and said inbound data, to

identify in at least one of said outbound data and said inbound data, relevant

commercial data that is to be stored in said data repository in accordance with said

rules in said policy data, and to cause said relevant commercial data to be stored in said

data repository (see., abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col

10, lines 1-67).

It is to be noted that Shwed fails to explicitly disclose that an analyzer, said analyzer being operable in conjunction with said policy data. However, Kater discloses a method/apparatus for analyzing the performance of a data processing system, particularly a distributed data processing, system, provide a system user with tools for analyzing and application running thereon (see., abstract, pages 1-11, [0096] and [0116]. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teaching of Shwed by including the limitation detailed above as taught by Kater because this would analyze performance of a data processing system.

As per claim 136 Shwed discloses a system/method for securing the flow of and selectively modifying packets in a computer network by controlling the inbound and outbound, the system comprising:

One or more workstations adapted for connection to a computer network, each workstation having a memory; providing an application stored in said memory of each workstation for transmitting outbound data to said computer network and receiving inbound data from said computer network; providing policy data containing rules specifying an appropriate encryption strength for outbound data, the encryption strength depending on the content of the data; and appropriate strength for the outbound data; wherein said analyzer controls transmission of said outbound data from said application in dependence upon said determination of an appropriate encryption strength; controlling transmission of said outbound data from said application in dependence

upon the determination of an appropriate encryption strength for the outbound data

(see., figs 1 and 2, abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10,

lines 1-67).

It is to be noted that Shwed further discloses an encryption strength see., col 2,

lines 37-40, col 13, lines 7-19, specifically wherein said the modification of

packets by, e.g., encryption of outbound packets....).

Policy data containing rules defining relevant commercial data which is to be stored in

said data repository (see., col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10,

lines 1-67); and

policy data to monitor at least one of said outbound data and said inbound data, to

identify in at least one of said outbound data and said inbound data, relevant

commercial data that is to be stored in said data repository in accordance with said

rules in said policy data, and to cause said relevant commercial data to be stored in said

data repository (see., abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col

10, lines 1-67).

It is to be noted that Shwed fails to explicitly disclose that an analyzer, said analyzer

being operable in conjunction with said policy data. However, Kater discloses a

method/apparatus for analyzing the performance of a data processing system,

particularly a distributed data processing, system, provide a system user with tools for

analyzing and application running thereon (see., abstract, pages 1-11, [0096] and

[0116]. Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to modify the teaching of Shwed by including the

limitation detailed above as taught by Kater because this would analyze performance of a data processing system.

As per claims 377 and 398 Shwed discloses a system/method for securing the flow of and selectively modifying packets in a computer network by controlling the inbound and outbound, the system comprising:

An application stored in said said memory of each workstation for transmitting outbound data to said computer network and receiving inbound data from said computer network;

policy data, containing rules which define whether or not verification is required for said digital certificate and in dependence on said one or more details of said signed data extracted (see., figs 1 and 2, abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67).

It is to be noted that Shwed further discloses an encryption strength or digital certificate (see., col 2, lines 37-40, col 13, lines 7-19, specifically wherein said the modification of packets by, e.g., encryption of outbound packets....).

Policy data containing rules defining relevant commercial data which is to be stored in said data repository (see., col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67); and

policy data to monitor at least one of said outbound data and said inbound data, to identify in at least one of said outbound data and said inbound data, relevant commercial data that is to be stored in said data repository in accordance with said rules in said policy data, and to cause said relevant commercial data to be stored in said

data repository (see., abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col

10, lines 1-67).

It is to be noted that Shwed fails to explicitly disclose that an analyzer, said analyzer

being operable in conjunction with said policy data. However, Kater discloses a

method/apparatus for analyzing the performance of a data processing system,

particularly a distributed data processing, system, provide a system user with tools for

analyzing and application running thereon (see., abstract, pages 1-11, [0096] and

[0116]. Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to modify the teaching of Shwed by including the

limitation detailed above as taught by Kater because this would analyze performance of

a data processing system.

As per claims 476 and 565 Shwed discloses a system/method for securing the flow of

and selectively modifying packets in a computer network by controlling the inbound and

outbound, the system comprising:

One or more workstations adapted for connection to a computer network, each

workstation having a memory; an application stored in said memory of each workstation

for transmitting outbound data to said computer network and receiving inbound data

from said computer network; policy data containing rules specifying an appropriate

encryption strength for outbound data, the encryption strength depending on the content

of the data; and appropriate strength for the outbound data; wherein said analyzer

controls transmission of said outbound data from said application in dependence upon

said determination of an appropriate encryption strength (see., figs 1 and 2, abstract, col

3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67).

It is to be noted that Shwed further discloses an encryption strength see., col 2,

lines 37-40, col 13, lines 7-19, specifically wherein said the modification of

packets by, e.g., encryption of outbound packets....).

Policy storage means, for storing policy data containing rules defining relevant

commercial data which is to be stored in said data repository (see., col 3, lines 8-67, col

4, lines 1-44, col 9, lines 1-67, col 10, lines 1-67); and

policy data to monitor at least one of said outbound data and said inbound data, to

identify in at least one of said outbound data and said inbound data, relevant

commercial data that is to be stored in said data repository in accordance with said

rules in said policy data, and to cause said relevant commercial data to be stored in said

data repository (see., abstract, col 3, lines 8-67, col 4, lines 1-44, col 9, lines 1-67, col

10, lines 1-67).

It is to be noted that Shwed fails to explicitly disclose that an analyzer, said analyzer

being operable in conjunction with said policy data. However, Kater discloses a

method/apparatus for analyzing the performance of a data processing system,

particularly a distributed data processing, system, provide a system user with tools for

analyzing and application running thereon (see., abstract, pages 1-11, [0096] and

[0116]. Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to modify the teaching of Shwed by including the

limitation detailed above as taught by Kater because this would analyze performance of a data processing system.

RESPONSE TO ARGUMENTS

6.   Applicant's arguments filed on 08/03/2006 have been fully considered but they are moot in view of new ground (s) of rejection.

Conclusion

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pierre E. Elisca whose telephone number is 571 272 6706. The examiner can normally be reached on 6:30 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571 272 6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PIERRE EDDY ELISCA
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600